

# 활성/백업 또는 활성/활성 시나리오에 대한 Umbrella SIG 터널 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

#### [배경 정보](#)

[Cisco Umbrella SIG 개요](#)

[Umbrella SIG 터널 대역폭 제한](#)

#### [Cisco Umbrella 포털 정보 보기](#)

[키 및 비밀 키 가져오기](#)

[조직 ID 가져오기](#)

#### [활성/백업 시나리오로 Umbrella SIG 터널 생성](#)

[1단계. SIG 자격 증명 기능 템플릿을 생성합니다.](#)

[2단계. SIG 기능 템플릿을 생성합니다.](#)

[3단계. 기본 터널에 대한 SIG 공급자를 선택합니다.](#)

[4단계. 보조 터널을 추가합니다.](#)

[5단계. 하나의 고가용성 쌍을 생성합니다.](#)

[6단계. 서비스 측 VPN 템플릿을 편집하여 서비스 경로를 삽입합니다.](#)

[활성/백업 시나리오에 대한 WAN 에지 라우터 컨피그레이션](#)

#### [활성/활성 시나리오로 Umbrella SIG 터널 생성](#)

[1단계. SIG 자격 증명 기능 템플릿을 생성합니다.](#)

[2단계. 2개의 루프백 인터페이스를 생성하여 SIG 터널을 연결합니다.](#)

[3단계. SIG 기능 템플릿을 생성합니다.](#)

---

## 소개

이 문서에서는 구성 방법을 설명합니다 Cisco Umbrella Secure Internet Gateway (SIG) IPsec이 있는 터널 Active/Active 및 Active/Standby.

## 사전 요구 사항

### 요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- Cisco Umbrella
- IPsec 협상

- Cisco SD-WAN(Software-defined Wide Area Network)

## 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco vManage 버전 20.4.2
- Cisco WAN Edge Router C1117-4PW\* 버전 17.4.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

### Cisco Umbrella SIG 개요

Cisco Umbrella 필수 기능을 통합하는 클라우드 기반 보안 서비스입니다.

Umbrella 보안 웹 게이트웨이, DNS 보안, 클라우드 제공 방화벽, 클라우드 액세스 보안 브로커 기능, 위협 인텔리전스를 통합합니다.

심층적인 검사 및 제어를 통해 사용 가능한 웹 정책을 준수하고 인터넷 위협으로부터 보호합니다.

SD-WAN 라우터는 대부분의 처리를 수행하여 엔터프라이즈 트래픽을 보호하는 SIG(Secure Internet Gateway)와 통합될 수 있습니다.

SIG가 설정되면 경로 또는 정책을 기반으로 하는 모든 클라이언트 트래픽이 SIG에 전달됩니다.

### Umbrella SIG 터널 대역폭 제한

에 대한 각 IPsec IKEv2 터널 Umbrella 헤드엔드는 약 250Mbps로 제한됩니다. 따라서 여러 개의 터널이 생성되어 트래픽을 로드 밸런싱하는 경우 더 높은 대역폭이 필요한 경우 이러한 제한을 극복합니다.

최대 4개 High Availability 터널 쌍을 생성할 수 있습니다.

## Cisco Umbrella 포털 정보 보기

SIG 통합을 진행하려면 Umbrella SIG 필수 패키지가 있는 계정이 필요합니다.

Understand what Umbrella licensing has been purchased for your organization and your overall utilization of the service.

### Umbrella Package

Current Package	License Start Date	License End Date	Number Of Seats
Umbrella SIG Advantage + Multi-Org + RBI L3	June 30, 2021	June 30, 2031	1

Information listed here is not authoritative in regard to seat count for certain customers. Customers under [Cisco's ELA](#) do not have a traditional concept of seat count limitation and, as such, this page does not accurately reflect those license types.

The values in the graph below = (number of DNS queries in applicable month / number of days in applicable month) / number of licensed Users

For questions about information seen here, or to change your licensing, contact your Cisco account manager or partner.

### Support

## 키 및 비밀 키 가져오기

키 및 비밀 키는 Umbrella Management API KEY (이 키는 '레거시 키' 아래에 있습니다.) 암호 키를 기억하지 않거나 저장하지 않은 경우 새로 고침 을 클릭합니다.

주의: Refresh(새로 고침) 버튼을 클릭하면 모든 디바이스에서 이 키에 대한 업데이트가 필요하지만, 사용 중인 디바이스가 있는 경우에는 업데이트를 사용하지 않는 것이 좋습니다.

Umbrella Management Key: 15 [Redacted] 36 Created: Jul 12, 2021

The API Key and secret pair enable you to manage the deployment for your different organizations. This includes the management of networks, roaming clients and other core-identity types.

Your Key: 15 [Redacted] 6

Check out the [documentation](#) for step by step instructions.

[DELETE](#) [REFRESH](#) [CLOSE](#)


## 조직 ID 가져오기

에 로그인하면 조직 ID를 쉽게 가져올 수 있습니다. Umbrella 브라우저 주소 표시줄에서 가져옵니다.

[https://dashboard.umbrella.com/o/\[Org ID\]/#/admin/apikeys](https://dashboard.umbrella.com/o/[Org ID]/#/admin/apikeys)

## 활성/백업 시나리오로 Umbrella SIG 터널 생성

참고: ECMP를 사용한 IPsec/GRE 터널 라우팅 및 로드 밸런싱: 이 기능은 vManage 20.4.1 이상에서 사용할 수 있으며, SIG 템플릿을 사용하여 애플리케이션 트래픽을 Cisco로 전달할 수 있습니다 Umbrella 또는 서드파티 SIG 제공자

 참고: Zscaler Automatic Provisioning 지원: vManage 20.5.1 이상에서 사용할 수 있는 이 기능은 Zscaler 파트너 API 자격 증명을 사용하여 Cisco SD-WAN 라우터에서 Zscaler로 터널을 자동으로 프로비저닝합니다.

SIG 자동 터널을 구성하려면 몇 가지 템플릿을 생성/업데이트해야 합니다.

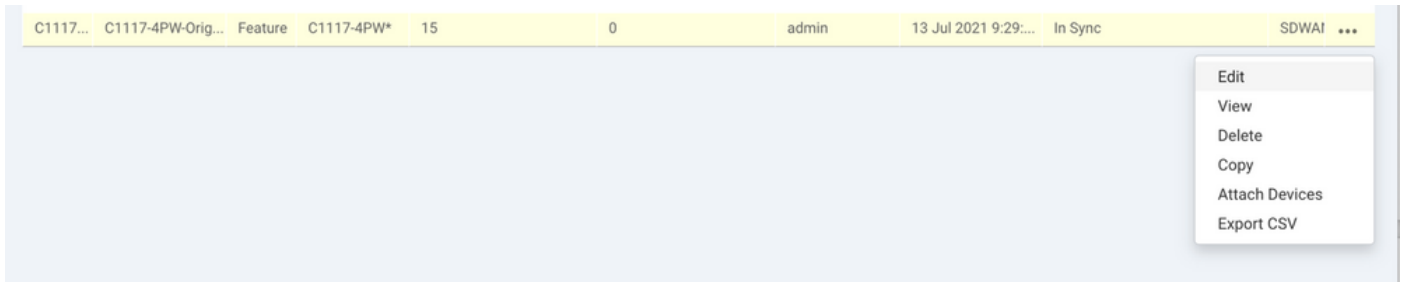
- SIG 자격 증명 기능 템플릿을 생성합니다.
- SIG 터널을 연결하기 위해 2개의 루프백 인터페이스를 생성합니다(둘 이상의 경우에만 적용 가능) Active 동시에 터널 - Active/Active 있습니다.
- SIG 기능 템플릿을 생성합니다.
- 서비스 측 VPN 템플릿을 편집하여 Service Route.

 참고: 모든 업스트림 디바이스에서 UDP 4500 및 500 포트를 허용해야 합니다.

템플릿 컨피그레이션은 Active/Backup 및 Active/Active 두 시나리오를 개별적으로 설명하고 노출하는 시나리오

1단계. SIG 자격 증명 기능 템플릿을 생성합니다.

기능 템플릿으로 이동하여 Edit.

C1117...	C1117-4PW-Orig...	Feature	C1117-4PW*	15	0	admin	13 Jul 2021 9:29:...	In Sync	SDWAN ...
									

의 조항 아래에 Additional templates, 클릭 Cisco SIG Credentials. 이 옵션이 이미지에 표시됩니다.

## Additional Templates

Global Template *	Factory_Default_Global_CISCO_Template ▼	
Cisco Banner	Choose... ▼	
Cisco SNMP	Choose... ▼	
CLI Add-On Template	Choose... ▼	
Policy	app-flow-visibility ▼	
Probes	Choose... ▼	
Security Policy	Choose... ▼	
Cisco SIG Credentials *	SIG-Credentials ▼	

템플릿에 이름과 설명을 지정합니다.

**CONFIGURATION | TEMPLATES**

**Device**    Feature

Feature Template > Cisco SIG Credentials > SIG-Credentials


**Device Type**    C1117-4PW\*


**Template Name**    SIG-Credentials


**Description**    SIG-Credentials


---

**Basic Details**

**SIG Provider**     Umbrella

**Organization ID**     [REDACTED]

**Registration Key**     [REDACTED]

**Secret**     [REDACTED]

[Get Keys](#)

2단계. SIG 기능 템플릿을 생성합니다.

기능 템플릿으로 이동한 다음 섹션 아래에서 **Transport & Management VPN Cisco Secure Internet Gateway** 기능 템플릿을 선택합니다.

**Transport & Management VPN**

Cisco VPN 0 \*    VPN0-C1117

Cisco Secure Internet Gateway    SIG-IPSEC-TUNNELS

Cisco VPN Interface Ethernet    VPN0-INTERFACE-GI-0-0-C1117

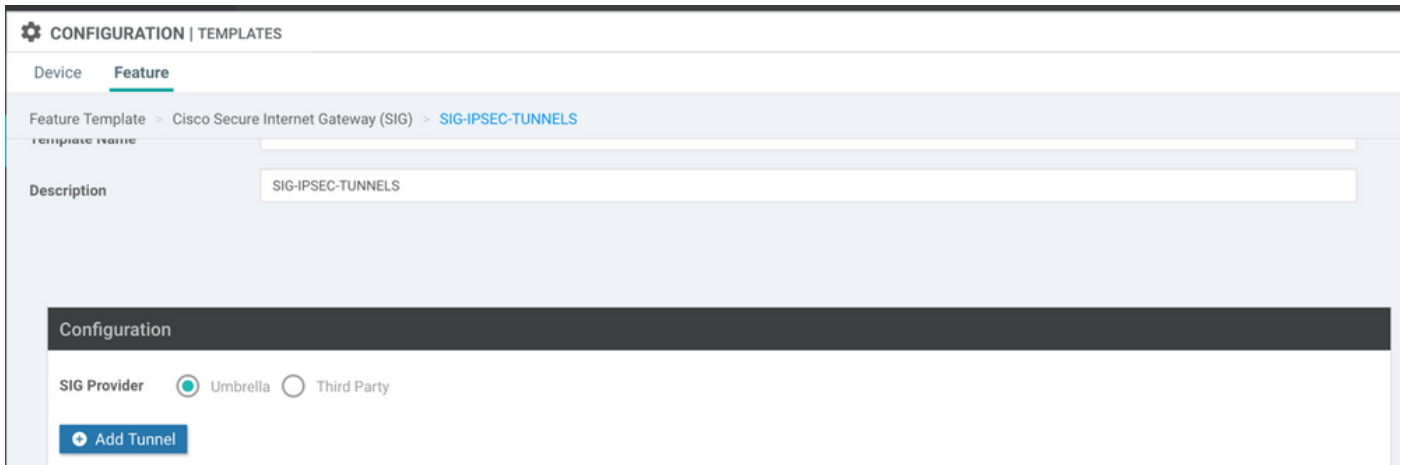
**Additional Cisco VPN 0 Templates**

- Cisco BGP
- Cisco OSPF
- Cisco OSPFv3
- Cisco Secure Internet Gateway
- Cisco VPN Interface Ethernet
- Cisco VPN Interface GRE
- Cisco VPN Interface IPsec
- VPN Interface Multilink Controller
- VPN Interface Ethernet PPPoE
- VPN Interface DSL IPoE
- VPN Interface DSL PPPoA
- VPN Interface DSL PPPoE
- VPN Interface SVI

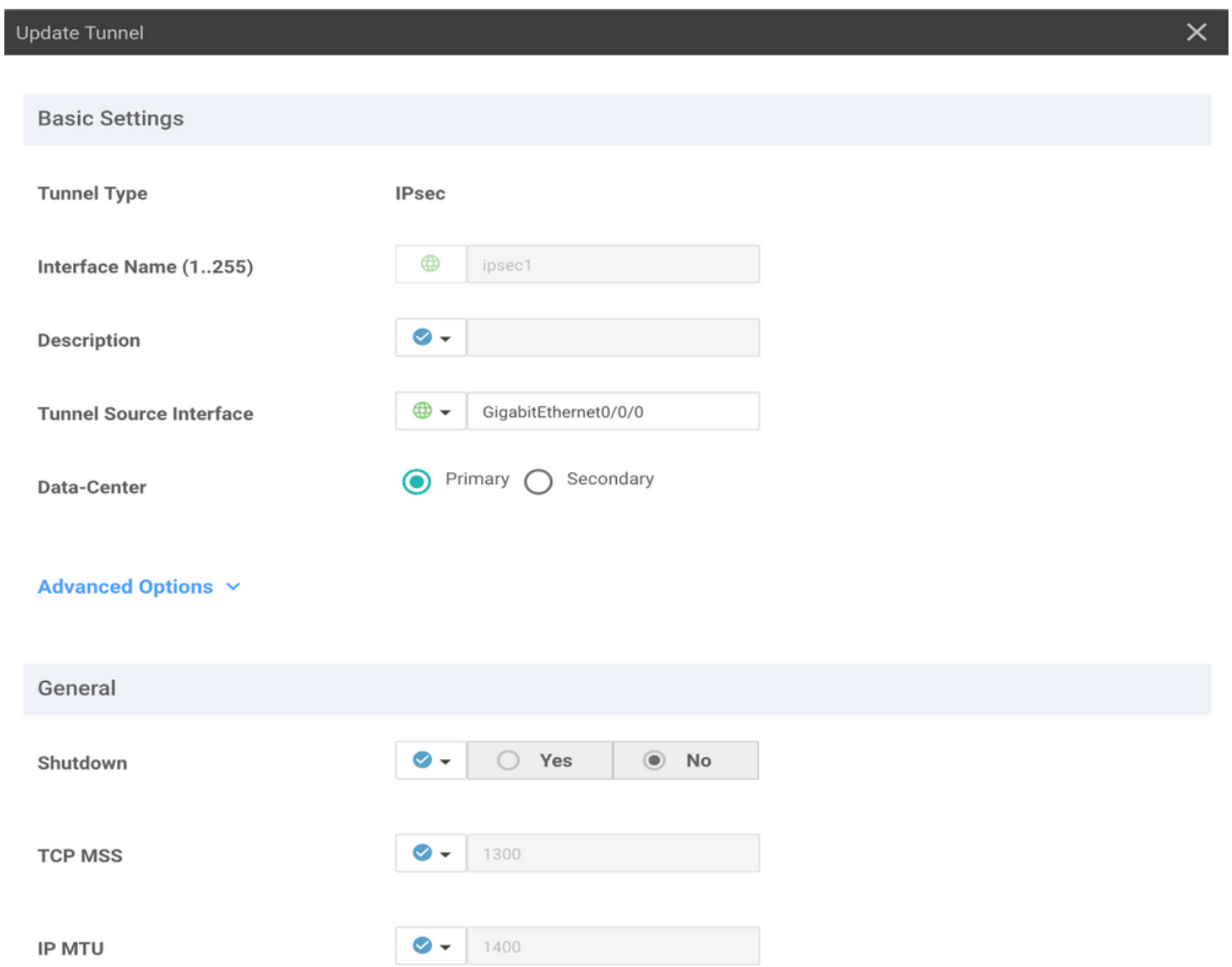
템플릿에 이름과 설명을 지정합니다.

3단계. 기본 터널에 대한 SIG 공급자를 선택합니다.

클릭 **Add Tunnel**.



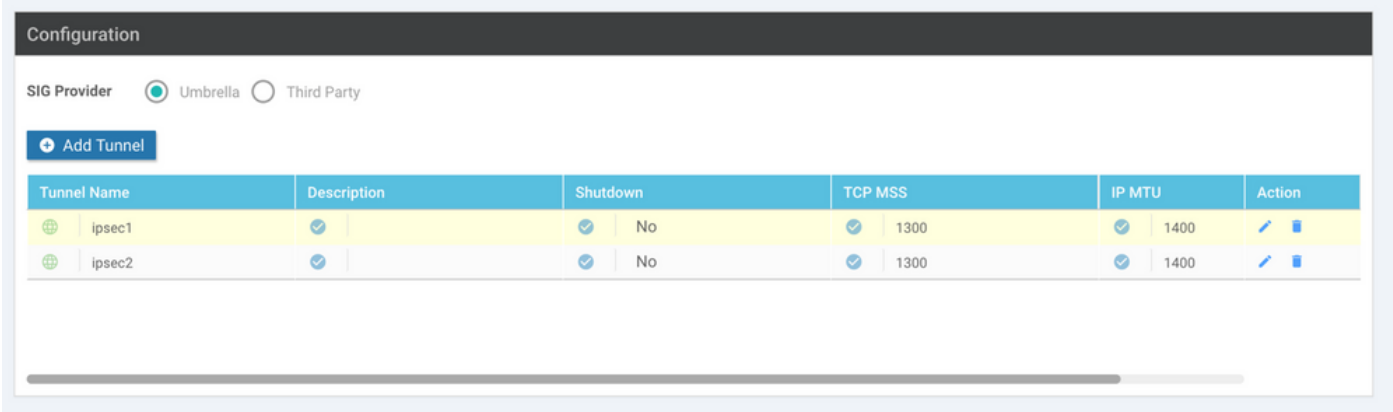
기본 세부 정보를 구성하고 유지 Data-Center 다음으로 Primary를 클릭한 다음 Add.



4단계. 보조 터널을 추가합니다.

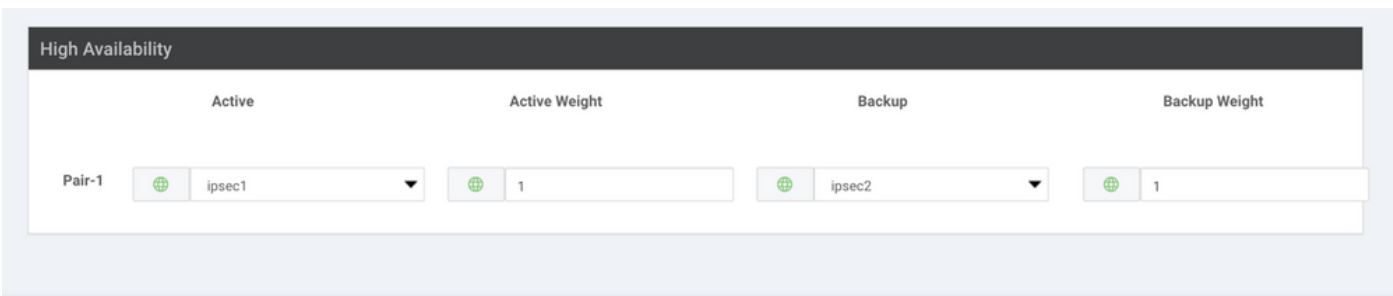
두 번째 터널 컨피그레이션을 추가합니다. Data-Center 다음으로 Secondary 이번에는 인터페이스 이름을 ipsec2로 지정합니다.


다음과 같이 vManage 컨피그레이션이 나타납니다.



5단계. 하나의고가용성 쌍을 생성합니다.

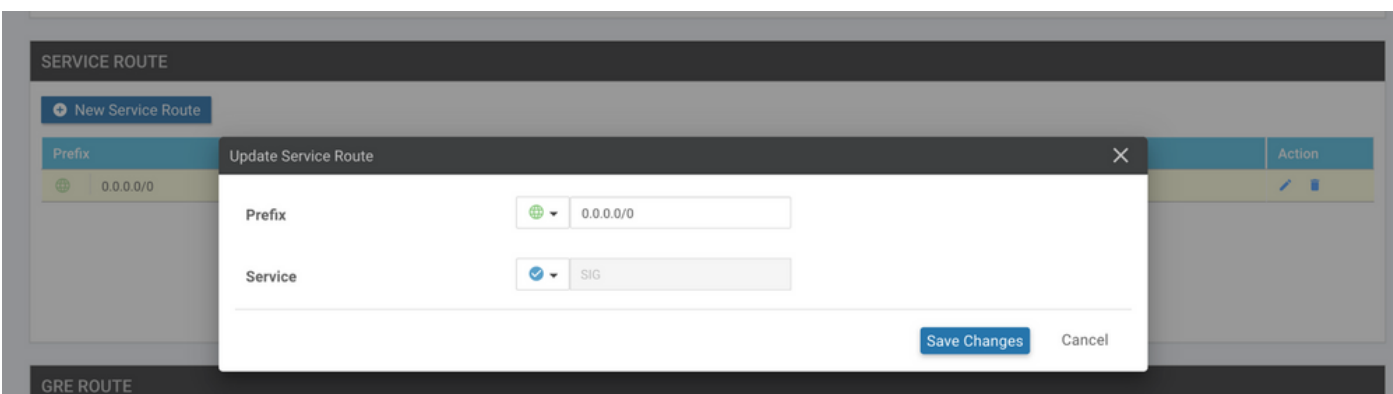
내부 **High Availability** 섹션에서 ipsec1을 Active로 선택하고 ipsec2 터널을 Backup으로 선택합니다.



 참고: 최대 4개 High Availability 터널 쌍 및 최대 4개의 활성 터널을 동시에 생성할 수 있습니다.

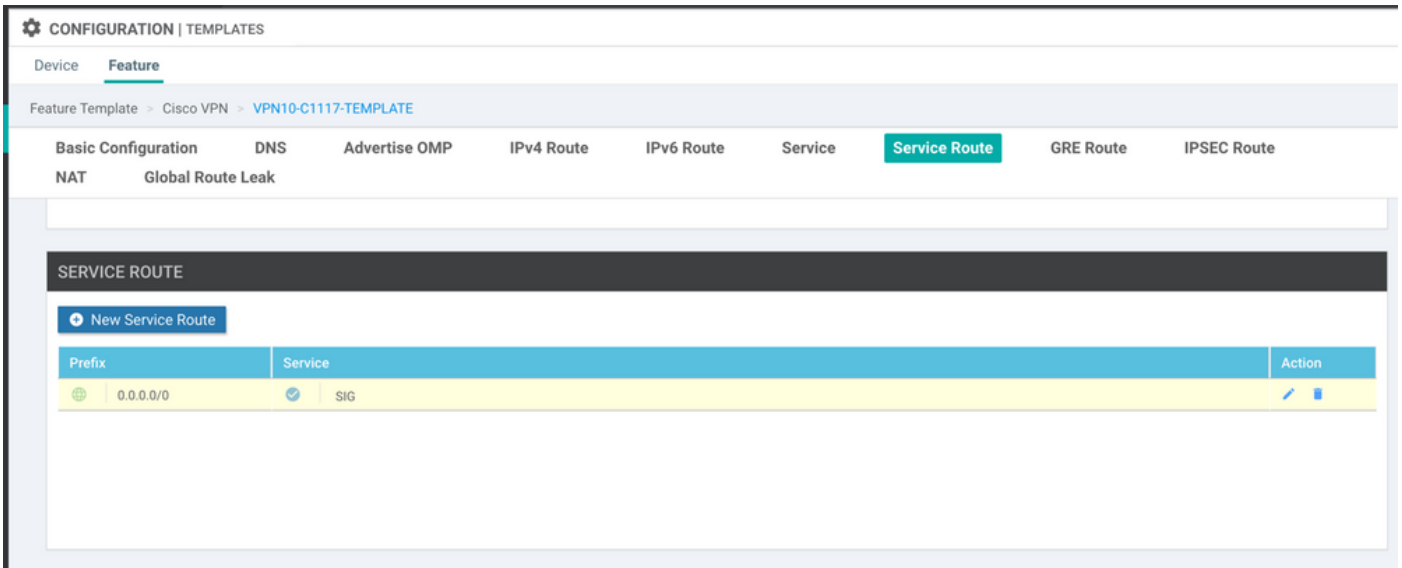
6단계. 서비스 측 VPN 템플릿을 편집하여 서비스 경로를 삽입합니다.

탐색: Service VPN 섹션 및, Service VPN 템플릿, 섹션으로 이동 Service Route SIG를 사용하여 0.0.0.0을 추가합니다. Service Route. 이 문서에서는 VRF/VPN 10을 사용합니다.



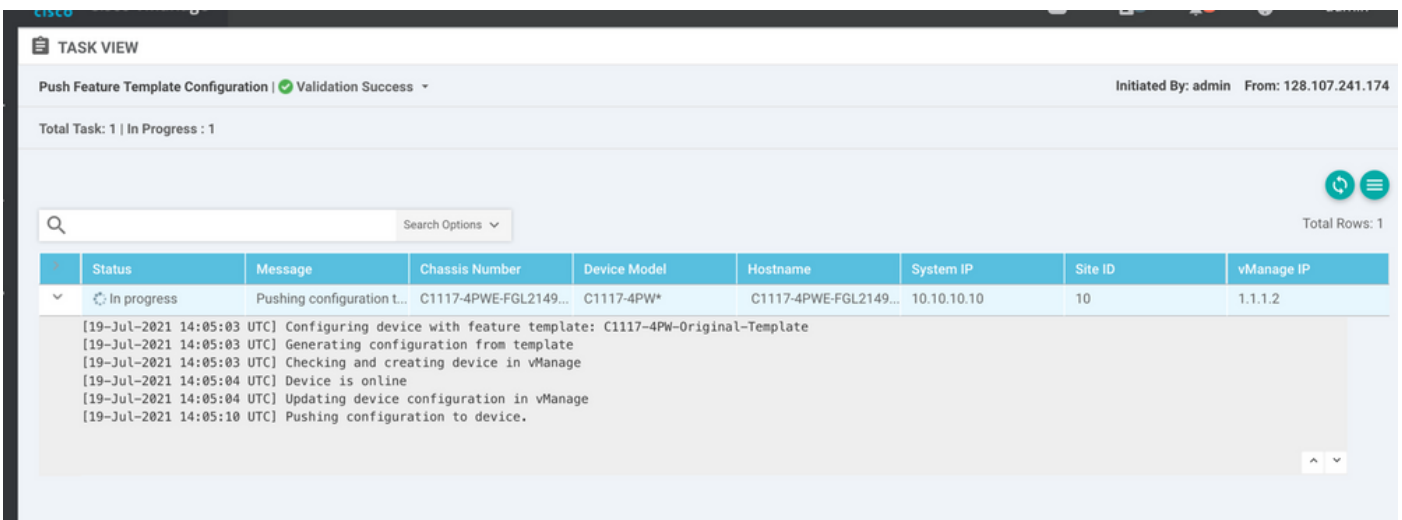
여기에 표시된 것처럼 0.0.0.0 SIG 경로가 표시됩니다.





 참고: 서비스 트래픽이 실제로 나가려면 NAT를 WAN 인터페이스에서 구성해야 합니다.

이 템플릿을 디바이스에 연결하고 컨피그레이션을 푸시합니다.



## 활성/백업 시나리오에 대한 WAN 에지 라우터 컨피그레이션

```

system
  host-name <HOSTNAME>
  system-ip <SYSTEM-IP>
  overlay-id 1
  site-id <SITE-ID>
  sp-organization-name <ORG-NAME>
  organization-name <SP-ORG-NAME>
  vbond <VBOND-IP> port 12346
!
secure-internet-gateway
  umbrella org-id <UMBRELLA-ORG-ID>
  umbrella api-key <UMBRELLA-API-KEY-INFO>

```

```

umbrella api-secret <UMBRELLA-SECRET-INFO>
!
sdwan
service sig vrf global
  ha-pairs
    interface-pair Tunnel100001 active-interface-weight 1 Tunnel100002 backup-interface-weight 1
  !
!
interface GigabitEthernet0/0/0
  tunnel-interface
    encapsulation ipsec weight 1
    no border
    color biz-internet
    no last-resort-circuit
    no low-bandwidth-link
    no vbond-as-stun-server
    vmanage-connection-preference 5
    port-hop
    carrier                                default
    nat-refresh-interval                   5
    hello-interval                         1000
    hello-tolerance                        12
    allow-service all
    no allow-service bgp
    allow-service dhcp
    allow-service dns
    allow-service icmp
    no allow-service sshd
    no allow-service netconf
    no allow-service ntp
    no allow-service ospf
    no allow-service stun
    allow-service https
    no allow-service snmp
    no allow-service bfd
  exit
exit
interface Tunnel100001
  tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-i
exit
interface Tunnel100002
  tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference secondary-dc source
exit
appqoe
  no tcpopt enable
!
security
  ipsec
    rekey                                86400
    replay-window                         512
    authentication-type sha1-hmac ah-sha1-hmac
  !
!
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname <DEVICE-HOSTNAME>
username admin privilege 15 secret 9 <SECRET-PASSWORD>
vrf definition 10
  rd 1:10
  address-family ipv4

```

```

    route-target export 1:10
    route-target import 1:10
    exit-address-family
    !
    address-family ipv6
    exit-address-family
    !
    !
vrf definition Mgmt-intf
    description Transport VPN
    rd      1:512
    address-family ipv4
    route-target export 1:512
    route-target import 1:512
    exit-address-family
    !
    address-family ipv6
    exit-address-family
    !
    !
ip sdwan route vrf 10 0.0.0.0/0 service sig
no ip http server
no ip http secure-server
no ip http ctc authentication
ip nat settings central-policy
vlan 10
exit
interface GigabitEthernet0/0/0
    no shutdown
    arp timeout 1200
    ip address dhcp client-id GigabitEthernet0/0/0
    no ip redirects
    ip dhcp client default-router distance 1
    ip mtu 1500
    load-interval 30
    mtu 1500
exit
interface GigabitEthernet0/1/0
    switchport access vlan 10
    switchport mode access
    no shutdown
exit
interface GigabitEthernet0/1/1
    switchport mode access
    no shutdown
exit
interface Vlan10
    no shutdown
    arp timeout 1200
    vrf forwarding 10
    ip address <VLAN-IP-ADDRESS> <MASK>
    ip mtu 1500
    ip nbar protocol-discovery
exit
interface Tunnel0
    no shutdown
    ip unnumbered GigabitEthernet0/0/0
    no ip redirects
    ipv6 unnumbered GigabitEthernet0/0/0
    no ipv6 redirects
    tunnel source GigabitEthernet0/0/0
    tunnel mode sdwan

```

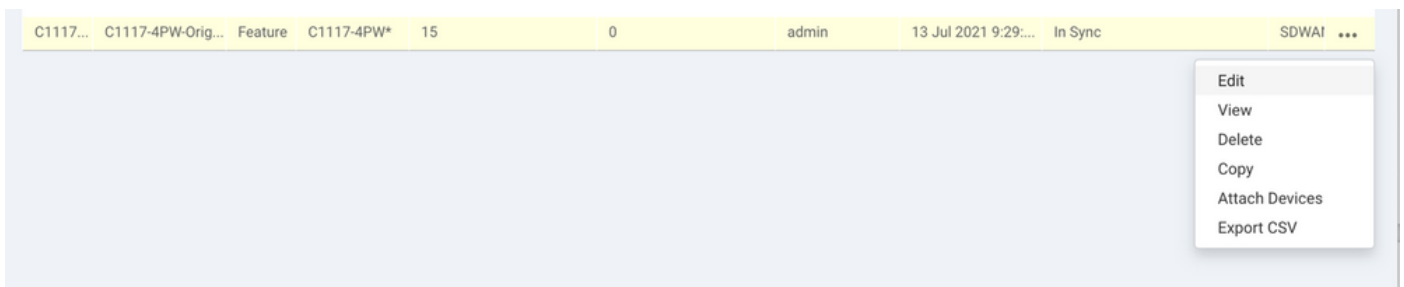
```
exit
interface Tunnel100001
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 ip mtu 1400
 tunnel source GigabitEthernet0/0/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec1-ipsec-profile
 tunnel vrf multiplexing
exit
interface Tunnel100002
 no shutdown
 ip unnumbered GigabitEthernet0/0/0
 ip mtu 1400
 tunnel source GigabitEthernet0/0/0
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec2-ipsec-profile
 tunnel vrf multiplexing
exit
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
logging console
no logging rate-limit
aaa authentication log in default local
aaa authorization exec default local
aaa session-id common
mac address-table aging-time 300
no crypto ikev2 diagnose error
crypto ikev2 policy policy1-global
 proposal p1-global
!
crypto ikev2 profile if-ipsec1-ikev2-profile
 no config-exchange request
 dpd 10 3 on-demand
 dynamic
 lifetime 86400
!
crypto ikev2 profile if-ipsec2-ikev2-profile
 no config-exchange request
 dpd 10 3 on-demand
 dynamic
 lifetime 86400
!
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 group 14 15 16
 integrity sha1 sha256 sha384 sha512
!
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
!
crypto ipsec transform-set if-ipsec2-ikev2-transform esp-gcm 256
 mode tunnel
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set ikev2-profile if-ipsec1-ikev2-profile
 set transform-set if-ipsec1-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
```

```
set security-association replay window-size 512
!  
crypto ipsec profile if-ipsec2-ipsec-profile  
set ikev2-profile if-ipsec2-ikev2-profile  
set transform-set if-ipsec2-ikev2-transform  
set security-association lifetime kilobytes disable  
set security-association lifetime seconds 3600  
set security-association replay window-size 512  
!  
no crypto isakmp diagnose error  
no network-clock revertive
```

## 활성/활성 시나리오로 Umbrella SIG 터널 생성


1단계. SIG 자격 증명 기능 템플릿을 생성합니다.

기능 템플릿으로 이동하여 **Edit**



의 조항 아래에 **Additional templates**, 선택 **Cisco SIG Credentials**. 옵션이 이미지에 표시됩니다.

## Additional Templates

Global Template *	Factory_Default_Global_CISCO_Template ▼	
Cisco Banner	Choose... ▼	
Cisco SNMP	Choose... ▼	
CLI Add-On Template	Choose... ▼	
Policy	app-flow-visibility ▼	
Probes	Choose... ▼	
Security Policy	Choose... ▼	
Cisco SIG Credentials *	SIG-Credentials ▼	

템플릿에 이름과 설명을 지정합니다.

**CONFIGURATION | TEMPLATES**

**Device**   Feature

Feature Template > Cisco SIG Credentials > SIG-Credentials

Device Type: C1117-4PW\*

Template Name: SIG-Credentials

Description: SIG-Credentials

---

**Basic Details**

SIG Provider:  Umbrella


Organization ID:


Registration Key:

Secret:

[Get Keys](#)

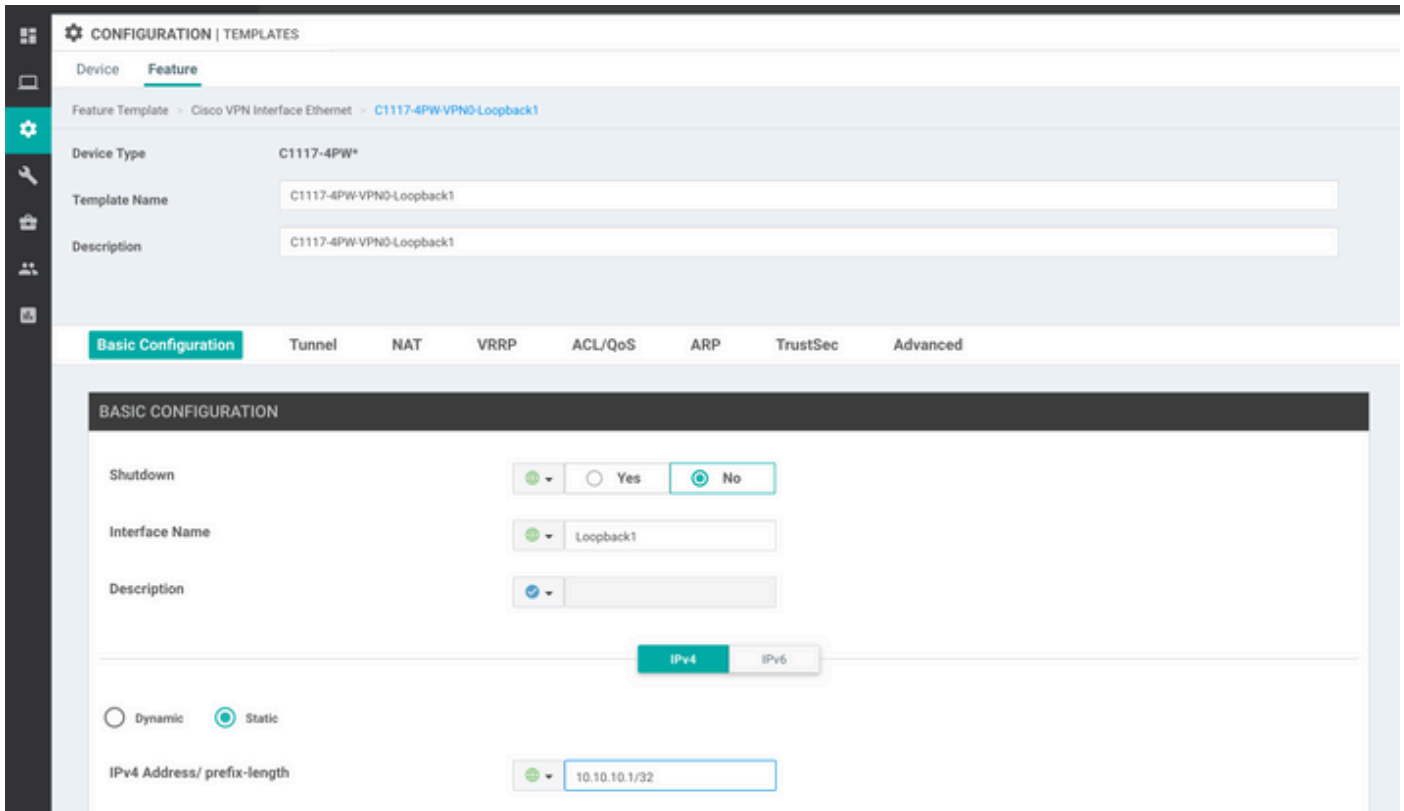
2단계. 2개의 루프백 인터페이스를 생성하여 SIG 터널을 연결합니다.

 참고: 액티브 모드에서 구성된 각 SIG 터널에 대해 루프백 인터페이스를 생성합니다. 각 터널에는 고유한 IKE ID가 필요하므로 이 인터페이스가 필요합니다.

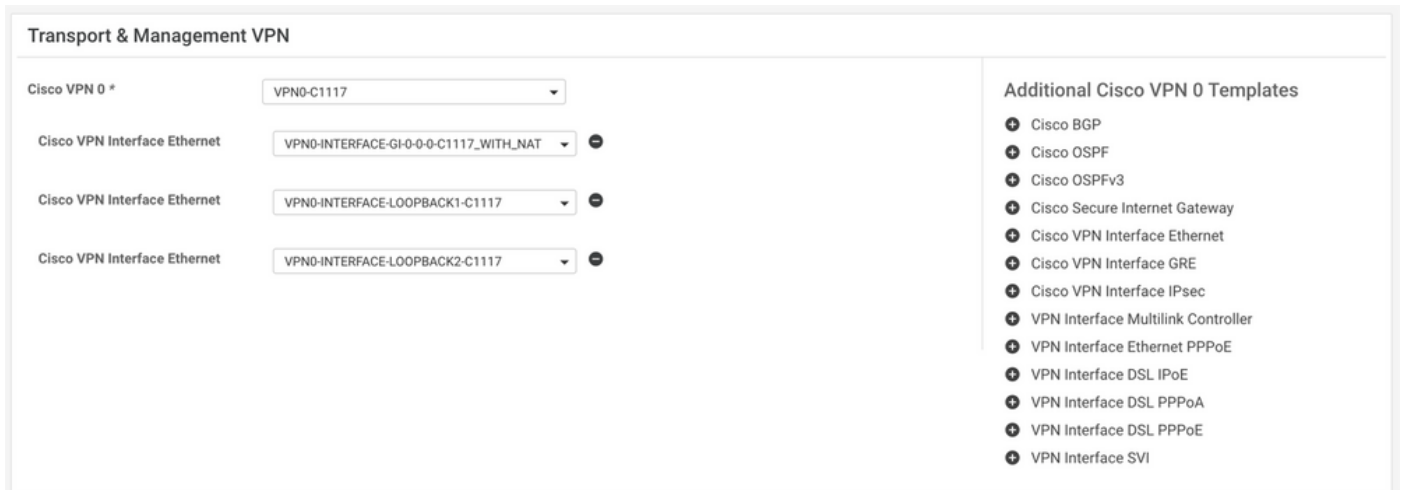
 참고: 이 시나리오는 활성/활성이므로 두 개의 루프백이 생성됩니다.

루프백에 대한 인터페이스 이름 및 IPv4 주소를 구성합니다.

 참고: 루프백에 대해 구성된 IP 주소는 더미 주소입니다.



두 번째 루프백 템플릿을 생성하여 디바이스 템플릿에 연결합니다. 디바이스 템플릿에는 두 개의 루프백 템플릿이 연결되어 있어야 합니다.



3단계. SIG 기능 템플릿을 생성합니다.

SIG 기능 템플릿으로 이동하고 섹션 아래에서 **Transport & Management VPN** 선택 **Cisco Secure Internet Gateway** 기능 템플릿.

4단계. 기본 터널의 SIG Provider(SIG 제공자)를 선택합니다.

클릭 **Add Tunnel**.



CONFIGURATION | TEMPLATES

Device **Feature**

Feature Template > Cisco Secure Internet Gateway (SIG) > SIG-IPSEC-TUNNELS

Template Name


Description SIG-IPSEC-TUNNELS

**Configuration**

SIG Provider  Umbrella  Third Party

**Add Tunnel**

기본 세부 정보를 구성하고 유지 Data-Center 다음으로 Primary.

 참고: Tunnel Source Interface 매개변수는 루프백(이 문서에서는 Loopback1)이고 Tunnel Route-via Interface는 물리적 인터페이스(이 문서에서는 GigabitEthernet0/0/0)입니다

Update Tunnel

**Basic Settings**

Tunnel Type IPsec

Interface Name (1..255) ipsec1

Description

Tunnel Source Interface Loopback1

Data-Center  Primary  Secondary

Tunnel Route-via Interface GigabitEthernet0/0/0

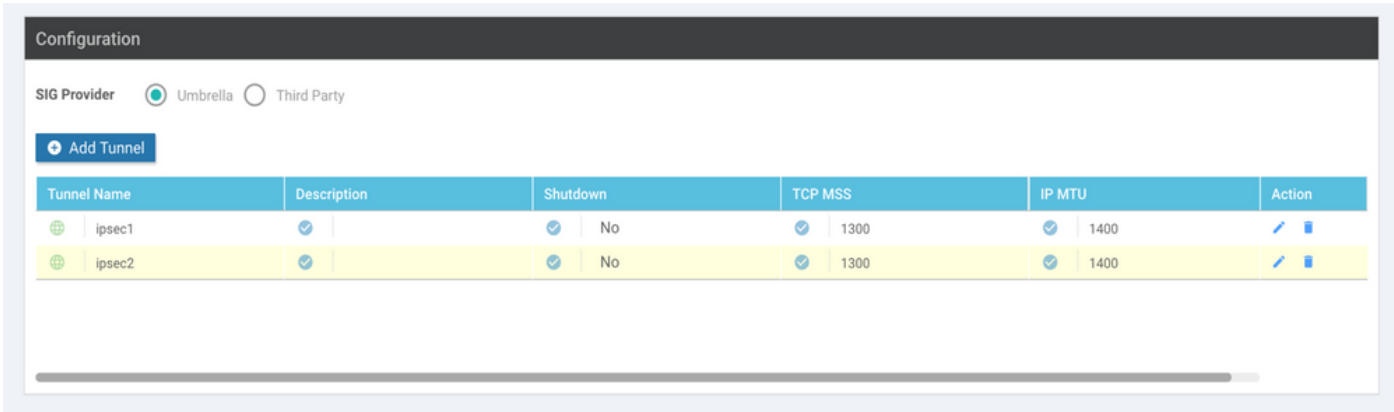
Advanced Options >

**Save Changes** Cancel

5단계. 보조 터널을 추가합니다.

두 번째 터널 컨피그레이션을 추가합니다. Data-Center 다음으로 Primary 인터페이스 이름은 ipsec2입니다.

다음과 같이 vManage 컨피그레이션이 나타납니다.

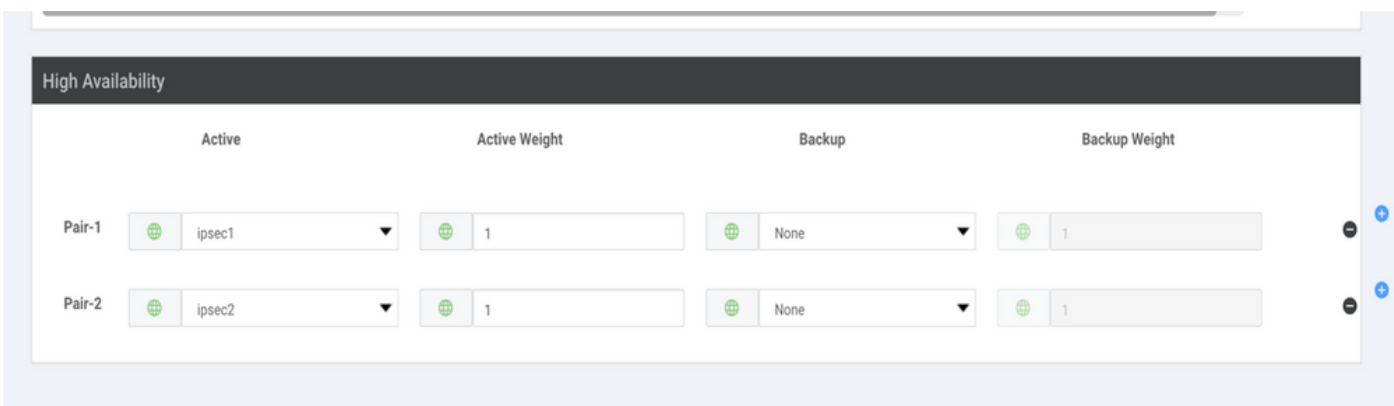


6단계. 두 개의고가용성 쌍을 생성합니다.

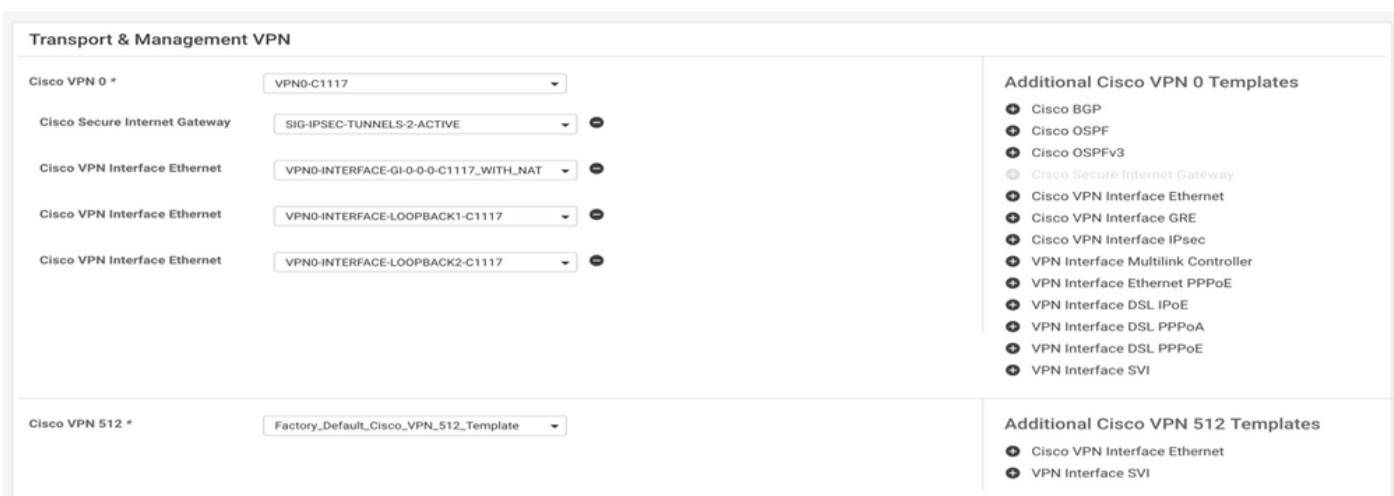
내부 High Availability 섹션, 2개 생성 High Availability 쌍.

- 첫 번째 HA 쌍에서 ipsec1을 Active(활성)로 선택하고 None 백업.
- 두 번째 HA 쌍에서 ipsec2를 Active(활성) 선택 None 백업을 위한 것입니다

에 대한 vManage 컨피그레이션 High Availability 다음과 같이 나타납니다.

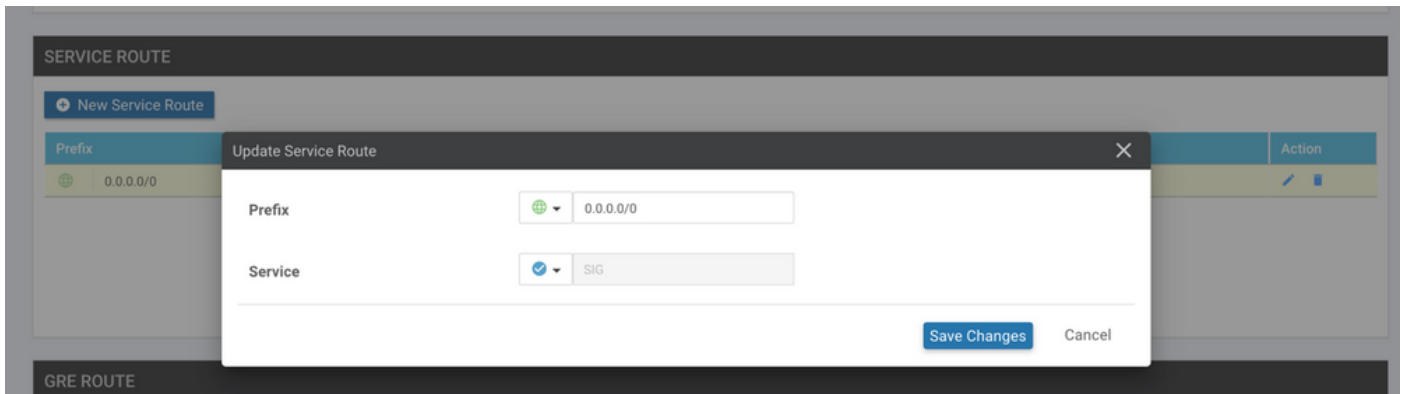


디바이스 템플릿에는 두 개의 루프백 템플릿과 SIG 기능 템플릿도 첨부되어 있습니다.



7단계. 서비스 측 VPN 템플릿을 편집하여 서비스 경로를 삽입합니다.

탐색: Service VPN 섹션 및 서비스 템플릿의 VPN에서 섹션으로 이동합니다 Service Route SIG를 사용하여 0.0.0.0을 추가합니다. Service Route



여기에 표시된 대로 0.0.0.0 SIG 경로가 나타납니다.

 참고: 서비스 트래픽이 실제로 나가려면 NAT를 WAN 인터페이스에서 구성해야 합니다.

이 템플릿을 디바이스에 연결하고 컨피그레이션을 푸시합니다.


### 액티브/액티브 시나리오에 대한 WAN 에지 라우터 컨피그레이션

```
system
 host-name <HOSTNAME>
 system-ip <SYSTEM-IP>
 overlay-id 1
 site-id <SITE-ID>
 sp-organization-name <ORG-NAME>
 organization-name <SP-ORG-NAME>
 vbond <VBOND-IP> port 12346
!
secure-internet-gateway
 umbrella org-id <UMBRELLA-ORG-ID>
 umbrella api-key <UMBRELLA-API-KEY-INFO>
 umbrella api-secret <UMBRELLA-SECRET-INFO>
!
sdwan
 service sig vrf global
  ha-pairs
  interface-pair Tunnel100001 active-interface-weight 1 None backup-interface-weight 1
  interface-pair Tunnel100002 active-interface-weight 1 None backup-interface-weight 1
!
interface GigabitEthernet0/0/0
 tunnel-interface
 encapsulation ipsec weight 1
 no border
 color biz-internet
 no last-resort-circuit
 no low-bandwidth-link
 no vbond-as-stun-server
 vmanage-connection-preference 5
 port-hop
 carrier default
 nat-refresh-interval 5
```

```
hello-interval 1000
hello-tolerance 12
allow-service all
no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
no allow-service snmp
no allow-service bfd
exit
exit
interface Tunnel100001
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-inte
exit
interface Tunnel100002
 tunnel-options tunnel-set secure-internet-gateway-umbrella tunnel-dc-preference primary-dc source-inte
exit
appqoe
no tcpopt enable
!
security
ipsec
rekey 86400
replay-window 512
authentication-type sha1-hmac ah-sha1-hmac
!
!
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname <DEVICE HOSTNAME>
username admin privilege 15 secret 9 <secret-password>
vrf definition 10
 rd 1:10
  address-family ipv4
  route-target export 1:10
  route-target import 1:10
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
!
vrf definition Mgmt-intf
 description Transport VPN
 rd 1:512
  address-family ipv4
  route-target export 1:512
  route-target import 1:512
  exit-address-family
!
  address-family ipv6
  exit-address-family
!
no ip source-route
```

```
ip sdwan route vrf 10 0.0.0.0/0 service sig
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload
ip nat translation tcp-timeout 3600
ip nat translation udp-timeout 60
ip nat settings central-policy
vlan 10
exit
interface GigabitEthernet0/0/0
no shutdown
arp timeout 1200
ip address dhcp client-id GigabitEthernet0/0/0
no ip redirects
ip dhcp client default-router distance 1
ip mtu 1500
ip nat outside
load-interval 30
mtu 1500
exit
interface GigabitEthernet0/1/0
switchport access vlan 10
switchport mode access
no shutdown
exit
interface Loopback1
no shutdown
arp timeout 1200
ip address 10.20.20.1 255.255.255.255
ip mtu 1500
exit
interface Loopback2
no shutdown
arp timeout 1200
ip address 10.10.10.1 255.255.255.255
ip mtu 1500
exit
interface Vlan10
no shutdown
arp timeout 1200
vrf forwarding 10
ip address 10.1.1.1 255.255.255.252
ip mtu 1500
ip nbar protocol-discovery
exit
interface Tunnel0
no shutdown
ip unnumbered GigabitEthernet0/0/0
no ip redirects
ipv6 unnumbered GigabitEthernet0/0/0
no ipv6 redirects
tunnel source GigabitEthernet0/0/0
tunnel mode sdwan
exit
interface Tunnel100001
no shutdown
ip unnumbered Loopback1
ip mtu 1400
tunnel source Loopback1
tunnel destination dynamic
tunnel mode ipsec ipv4
tunnel protection ipsec profile if-ipsec1-ipsec-profile
tunnel vrf multiplexing
tunnel route-via GigabitEthernet0/0/0 mandatory
```

```
exit
interface Tunnel100002
 no shutdown
 ip unnumbered Loopback2
 ip mtu 1400
 tunnel source Loopback2
 tunnel destination dynamic
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile if-ipsec2-ipsec-profile
 tunnel vrf multiplexing
 tunnel route-via GigabitEthernet0/0/0 mandatory
exit
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging buffered 512000
logging console
no logging rate-limit
aaa authentication log in default local
aaa authorization exec default local
aaa session-id common
mac address-table aging-time 300
no crypto ikev2 diagnose error
crypto ikev2 policy policy1-global
proposal p1-global
!
crypto ikev2 profile if-ipsec1-ikev2-profile
 no config-exchange request
 dpd 10 3 on-demand
 dynamic
 lifetime 86400
!
crypto ikev2 profile if-ipsec2-ikev2-profile
 no config-exchange request
 dpd 10 3 on-demand
 dynamic
 lifetime 86400
!
crypto ikev2 proposal p1-global
 encryption aes-cbc-128 aes-cbc-256
 group 14 15 16
 integrity sha1 sha256 sha384 sha512
!
crypto ipsec transform-set if-ipsec1-ikev2-transform esp-gcm 256
 mode tunnel
!
crypto ipsec transform-set if-ipsec2-ikev2-transform esp-gcm 256
 mode tunnel
!
crypto ipsec profile if-ipsec1-ipsec-profile
 set ikev2-profile if-ipsec1-ikev2-profile
 set transform-set if-ipsec1-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
crypto ipsec profile if-ipsec2-ipsec-profile
 set ikev2-profile if-ipsec2-ikev2-profile
 set transform-set if-ipsec2-ikev2-transform
 set security-association lifetime kilobytes disable
 set security-association lifetime seconds 3600
 set security-association replay window-size 512
!
```

 참고: 이 문서는 Umbrella에 중점을 두지만 Azure 및 서드파티 SIG 터널에도 동일한 시나리오가 적용됩니다.

## 다음을 확인합니다.

### 활성/백업 시나리오 확인

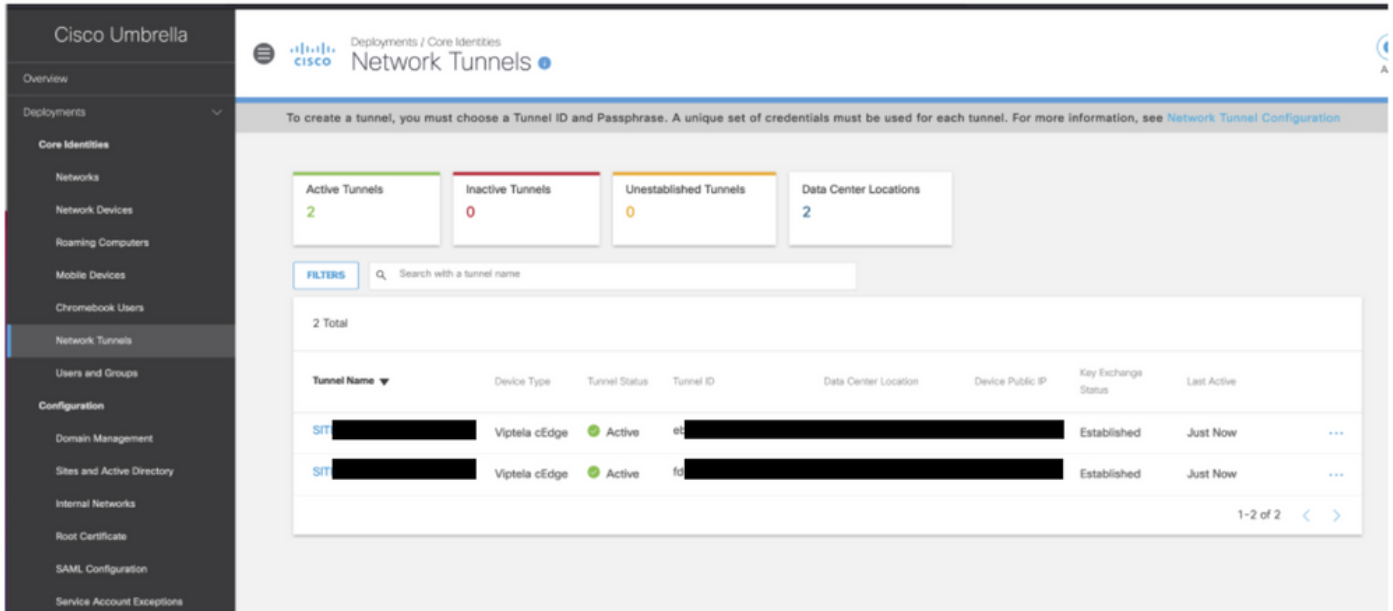
vManage에서 SIG IPSec 터널의 상태를 모니터링할 수 있습니다. 탐색 **Monitor > Network**, 원하는 WAN 에지 디바이스를 선택합니다.

다음을 클릭합니다. **Interfaces** 왼쪽에 탭, 디바이스의 모든 인터페이스 목록이 표시됩니다. 여기에는 ipsec1 및 ipsec2 인터페이스가 포함됩니다.

이 그림에서는 ipsec1 터널이 모든 트래픽을 전달하며 ipsec2가 트래픽을 전달하지 않음을 보여 줍니다.



Cisco에서 터널을 확인할 수도 있습니다 **Umbrella** 이미지에 포털이 표시됩니다.



이 `show sdwan secure-internet-gateway tunnels` 명령을 실행하여 터널 정보를 표시합니다.

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
```

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	540798313	SITE10SYS10x10x10x10IFTunnel100001	st-tun-create-notif	200	create-tunnel
Tunnel100002	540798314	SITE10SYS10x10x10x10IFTunnel100002	st-tun-create-notif	200	create-tunnel

이 `show endpoint-tracker` 및 `show ip sla summary` 명령을 실행하여 자동 생성된 추적기 및 SLA에 대한 정보를 표시합니다.

```
cEdge_Site1_East_01#show endpoint-tracker
```

Interface	Record Name	Status	RTT in msec	Probe ID	Next Hop
Tunnel100001	#SIGL7#AUTO#TRACKER	Up	8	14	None
Tunnel100002	#SIGL7#AUTO#TRACKER	Up	2	12	None

```
cEdge_Site1_East_01#show ip sla summary
```

IPSLAs Latest Operation Summary  
Codes: \* active, ^ inactive, ~ pending  
All Stats are in milliseconds. Stats with u are in microseconds

ID	Type	Destination	Stats	Return Code	Last Run
*12	http	10.10.10.10	RTT=6	OK	8 seconds ago
*14	http	10.10.10.10	RTT=17	OK	3 seconds ago

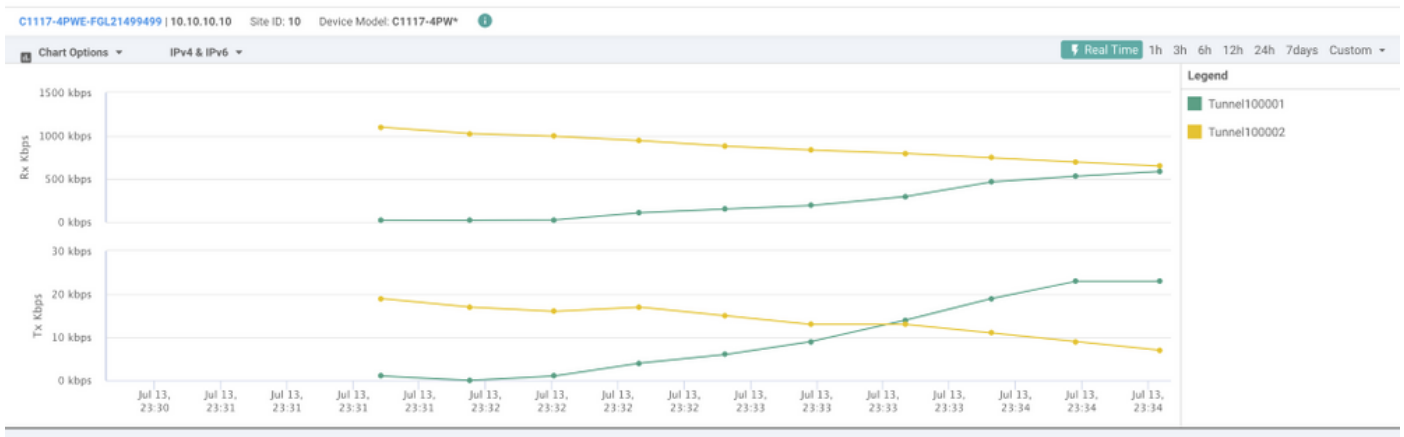


## 활성/활성 시나리오 확인

vManage에서는 SIG IPsec 터널의 상태를 모니터링할 수 있습니다. 탐색 **Monitor > Network**, 원하는 WAN 에지 디바이스를 선택합니다.

다음을 클릭합니다. **Interfaces** 왼쪽에 탭 - 디바이스의 모든 인터페이스 목록이 표시됩니다. 여기에는 ipsec1 및 ipsec2 인터페이스가 포함됩니다.

이 그림에서는 ipsec1 및 ipsec2 터널 모두 트래픽을 전달하는 것을 보여 줍니다.



이 `show sdwan secure-internet-gateway tunnels` 명령을 실행하여 터널 정보를 표시합니다.

```
C1117-4PWE-FGL21499499#show sdwan secure-internet-gateway tunnels
```

TUNNEL IF NAME	TUNNEL ID	TUNNEL NAME	FSM STATE	API HTTP CODE	LAST SUCCESSFUL REQ
Tunnel100001	540798313	SITE10SYS10x10x10x10IFTunnel100001	st-tun-create-notif	200	create-tunnel
Tunnel100002	540798314	SITE10SYS10x10x10x10IFTunnel100002	st-tun-create-notif	200	create-tunnel

이 `show endpoint-tracker` 및 `show ip sla summary` 명령을 실행하여 자동 생성된 추적기 및 SLA에 대한 정보를 표시합니다.

```
cEdge_Site1_East_01#show endpoint-tracker
```

Interface	Record Name	Status	RTT in msec	Probe ID	Next Hop
Tunnel100001	#SIGL7#AUTO#TRACKER	Up	8	14	None
Tunnel100002	#SIGL7#AUTO#TRACKER	Up	2	12	None

```
cEdge_Site1_East_01#show ip sla summary
```

IPSLAs Latest Operation Summary  
Codes: \* active, ^ inactive, ~ pending  
All Stats are in milliseconds. Stats with u are in microseconds

ID	Type	Destination	Stats	Return	Last
----	------	-------------	-------	--------	------

				Code	Run
*12	http	10.10.10.10	RTT=6	OK	8 seconds ago
*14	http	10.10.10.10	RTT=17	OK	3 seconds ago

## 관련 정보

- [보안 인터넷 게이트웨이와 장치 통합 - Cisco IOS® XE Release 17.x](#)
- [http://Network 터널 컨피그레이션 - Umbrella SIG](#)
- [Umbrella 시작하기](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.